United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

IN RE INTEL CORPORATION SECURITIES LITIGATION

CASE NO. 18-cv-00507-YGR

ORDER GRANTING MOTION TO DISMISS WITH LEAVE TO AMEND

Re: Dkt. No. 67

Lead plaintiff Louisiana Sheriffs' Pension & Relief Fund brings this securities class action litigation alleging false and misleading statements and omissions between October 27, 2018 and January 9, 2018 (the "Class Period"), against defendants Intel Corporation ("Intel," or the "Company"), and three individual defendants, namely Brian M. Krzanich (former Chief Executive Officer or "CEO"), Robert H. Swan (Chief Financial Officer or "CFO"), and Navin Shenoy (Executive Vice-President). Specifically, plaintiff raises the following causes of action: (i) violation of Section 10(b) of the Securities Exchange Act ("Exchange Act") against all defendants and Rule 10b-5 promulgated thereunder and (ii) violation of Section 20(a) of the Exchange Act against the individual defendants.

Defendants have filed a motion to dismiss, pursuant to Federal Rules of Civil Procedure 8(a), 9(b), and 12(b)(6), and the Private Securities Litigation Reform Act of 1995 ("PSLRA"). (*See* Defendants' Motion to Dismiss Consolidated Complaint ("MTD"), Dkt. No. 67.) Therein, defendants challenge plaintiff's Section 10(b) claim on two grounds. First, plaintiff fails to identify any statements which were false or misleading when made. Second, plaintiff has not established a strong inference of scienter. With regard to plaintiff's Section 20(a) claim against the individual defendants, defendants argue that plaintiff has not shown an underlying predicate violation under Section 10(b) or facts establishing the element of control as to Shenoy.

Having considered the papers submitted and the pleadings in this action, the hearing held on March 12, 2019, and for the reasons set forth below, the Court hereby **GRANTS** the motion to dismiss **WITH LEAVE TO AMEND**.

I. BACKGROUND

The facts at issue in this case, as pleaded in plaintiff's Consolidated Class Action Complaint ("CCAC"), (Dkt. No. 57), are well known to the parties. Relevant allegations from the CCAC, and facts based on judicially noticeable documents and documents incorporated by reference in the CCAC, are set forth below.

A. INTEL'S SEMICONDUCTOR PRODUCTS

Intel is one of the world's largest manufacturers of processors, chipsets, and related computer components. (CCAC ¶ 2.) Intel provides processors to more than 90 percent of all personal computers and servers supporting the internet and business operations. (*Id*.) Sales of processors and chipsets account for over 80 percent of Intel's total annual revenue. (*Id*.) These components are integral to the functioning of computers, servers, smartphones, tablets, and networking and communications products. (*Id*. ¶ 23.)

Specifically, Intel typically offers its products as "platforms." (*Id*. ¶ 25.) A platform consists of a microprocessor and chipset. (*Id*.) A microprocessor is a computer processor on a microchip and is the main component of all computers, often referred to as the "brain" of a computer. (*Id*.) It is critical to a computer's performance and processing speed. (*Id*.) The key functional block of a microprocessor is the Central Processing Unit, or "CPU." (*Id*.)[1] A chipset is a computer's "nervous system," sending data between the microprocessor and inputs, displays, and storage devices such as keyboard, mouse, and monitor. (*Id*. ¶ 26.) The chipset performs essential logic functions and controls the access between the CPU and main memory. (*Id*.) Intel's success depends on continuously improving the power, speed, and performance of its processors. (*Id*. ¶ 32.)

[1] Although technically distinct components, the terms processors, chips, and CPUs are often used interchangeably. *Id*. ¶ 25 n. 2.

Due to the "widespread use" of Intel's products and the "high profile of [its] commercial security products," Intel has warned its investors of associated cybersecurity and privacy risks. In its 2016 10-K filed in February 2017, Intel stated:

> [M]alicious hackers may attempt to gain unauthorized access and corrupt the processes of hardware and software products that we manufacture . . . . [O]ur products . . . are a frequent target of computer hackers and organizations that tend to sabotage, take control of, or otherwise corrupt our . . . products . . . . We believe such attempts are increasing in number and in technical sophistication. From time to time, we encounter intrusions or unauthorized access to our . . . products . . . . While we seek to detect and investigate all unauthorized attempts and attacks against our . . . products, . . . we remain potentially vulnerable to additional known or unknown threats. Such incidents, whether successful or unsuccessful, could result in our incurring significant costs related to, for example, rebuilding internal systems, reduced inventory value, providing modifications to our products and services, defending against litigation, responding to regulatory inquiries or actions, paying damages, or taking other remedial steps with respect to third parties.

(Defendants' Motion to Dismiss Consolidated Complaint; Errata ("Amended Exhibit 9" or "2016 Form 10-K") at 20, Dkt. No. 81.)[2] Moreover, product webpages include an express warning that "[n]o computer system can be absolutely secure." (Xio Decl. Exh. 17 at ECF p. 5.)

B. SPECTRE AND MELTDOWN VULNERABILITIES

On June 1, 2017, an analyst from Google's Project Zero—which is dedicated to finding vulnerabilities in Google software and any software or hardware employed by its users—notified Intel and two other chipmakers (Advanced Micro Devices, Inc. and ARM Holdings) of a "CPU security issue that affects processors," later known as "Spectre." (*Id*. ¶ 52; *see also id*. ¶ 45.) Later in June, Google Project Zero identified a second vulnerability that became known as "Meltdown" and which "allows a hacker to move the highly sensitive data stored in kernel memory to the cache memory." (*Id*. ¶ 55; *see also id*. ¶ 54.)[3] While the two vulnerabilities

---

[2] As discussed below, (*see infra* at 9 n.8, 11), the 2016 Form 10-K is a subject of defendants' Request for Consideration of Documents Incorporated into Consolidated Complaint and for Judicial Notice in Support of Motion to Dismiss Consolidated Complaint, Dkt. No. 68. *See also* Declaration of Xiao Wang in Support of Defendants' Request for Consideration of Documents Incorporated Into Consolidated Complaint and for Judicial Notice in Support of Motion to Dismiss Consolidated Complaint ("Xiao Decl."), Dkt. No. 67-1. Defendants inadvertently filed Intel's 2017 Form 10-K (*see* Xiao Decl. Exh. 9, Dkt. No. 67-10), but subsequently filed an errata attaching Intel's 2016 Form 10-K.

[3] "Kernel memory" is "a protected area of memory used by the operating system and

present different security risks, they both allow a hacker to "trick" a computer into moving sensitive information into the cache memory, where the hacker can access the information, including secret keys, passwords, and any other sensitive information stored on a computer. (*Id*. ¶ 54.) Spectre and Meltdown impact nearly every Intel processor produced since 1995—approximately 90 percent of all Intel platforms. (*Id*. ¶ 56.) In or around September and December of 2017, additional researchers independently reported to Intel their discovery of the flaws. (*Id*. ¶¶ 57, 58.) Despite these reports, the CCAC alleges no actual reported hacks resulting from the Spectre and Meltdown vulnerabilities.[4]

After Google Project Zero informed Intel of the Spectre and Meltdown vulnerabilities in June 2017, the Company conducted a "detailed analysis" of the vulnerabilities in June and July of 2017 that confirmed their existence. (*Id*. ¶ 64.) Pursuant to Google Project Zero's standard protocol, whereby it affords companies like Intel 90 days to either disclose or remediate a threat, (*id*. ¶ 46),[5] the securities vulnerabilities were supposed to be publicly disclosed in early September 2017. (*Id*. ¶ 65.) However, an unusual "deadline grace" was granted to Intel on August 7, 2017, extending the 90-day disclosure deadline. (*Id*.) Accordingly, Intel and other market participants planned to disclose simultaneously the existence of the vulnerabilities and deploy mitigations on January 9, 2018. (*Id*. ¶ 105; *see also id*. ¶ 6.) This disclosure process was consistent with the publicly-known "common practice" of "keep[ing] the news [of security vulnerabilities] from the public so hackers [cannot] take advantage of [such] flaws before they [a]re fixed." (Xiao Decl. Exh. 4 at 2; *see also id.* Exh. 5 at 2 ("[T]he custom is to give vendors a few months to fix the problem before it goes public and bad guys have a chance to exploit it.").)

---

contains a computer's most confidential information, such as secret encryption keys, passwords[,] and other sensitive information." *Id*. ¶ 50. The "cache memory" is "less secure," and data in the cache memory is "more vulnerable to unauthorized access." *Id*. ¶ 44.

[4] Indeed, at oral argument, plaintiff's counsel indicated that these researchers and the researchers at Google Project Zero were the only known individuals who "cracked the code." *See* Transcript of March 12, 2019 Proceedings ("Tr.") at 6:15–18, Dkt. No. 86. Plaintiff's efforts at oral argument to characterize the researchers' efforts as "hacks" are unavailing.

[5] Only in "extreme circumstance" will Google Project Zero extend the 90-day deadline. *Id*. ¶ 47.

Intel worked for "months" with a limited group of industry collaborators attempting to develop mitigations, test them, and prepare releases. (*Id*. ¶ 66 (emphasis removed).) Its efforts involved "multiple microprocessor vendors, operating system vendors[,] and [Original Equipment Manufacturers ('OEM')] around the world" working to understand the issue and "to develop the system software updates, to develop the firmware[,] and to integrate and test those things." (*Id*. ¶ 110 (internal quotation marks omitted).)[6]

In the meantime, Intel did not inform the National Security Agency, the Department of Homeland Security, the United States Computer Emergency Readiness Team ("US-CERT"), or the CERT Coordination Center ("CERT/CC") about Spectre or Meltdown even though such government agencies rely on computers, servers, and networks powered by Intel processors. (*Id*. ¶¶ 67, 70.) However, the Company informed select clients in or around November 2017. (*Id*. ¶ 70.)

Given the threat that Spectre and Meltdown posed to almost all of Intel's microprocessors, a former Intel security engineer has no doubt that Intel's CEO would have been informed of the problems. (*Id*. ¶ 73.) Moreover, given that Spectre and Meltdown crossed so many product lines at Intel, the engineer expects that Intel's CEO and CFO would have reviewed and approved the disclosure plan for Spectre and Meltdown. (*Id*.) Because the Data Center Group was one of the units directly impacted, defendant Shenoy, as head of the same, would have participated in discussions regarding potential mitigations and their impacts on performance and would have made the "final call" on which mitigations to deploy. (*Id*. ¶ 75 (internal quotation marks omitted).) Shenoy and other senior business leaders, in turn, would have provided Krzanich, Swan, and other corporate executives with weekly or bi-weekly reports. (*Id*.)

On November 29, 2017, the same day that Intel informed its OEM partners about Spectre, Krzanich sold 890,000 shares of Intel stock for nearly $40 million, netting almost $25 million in profits. (*Id*. ¶ 100.) This amounted to 100% of the shares he could sell under the Company's

[6] OEMs make (i) computer systems, (ii) cellular handsets and handheld computing devices, and (iii) networking communications equipment. *Id*. ¶ 29(a).

bylaws, 80% of his total personal Intel holdings, and more than ten times greater than any other sale in the previous two years. (*Id*.) Krzanich sold his shares under a Rule 10b5-1 plan that he modified 30 days before he unloaded his shares. (*Id*. ¶ 102.)

Although Intel and market participants had initially planned to disclose the existence of the vulnerabilities and deploy the mitigations on January 9, 2018, on January 2, 2018, British technology website *The Register* reported that researchers had identified Meltdown. (*Id*. ¶ 105.) On this news, Intel's stock plunged, wiping out billions of dollars in market capitalization. (*Id*. ¶ 106.) The following day, Intel admitted that it had previously been made aware of Spectre and Meltdown but explained that, due to its "commit[ment] to the industry best practice of responsible disclosure of potential security issues," it "had planned to disclose the issue next week when more software and firmware updates w[ould] be available." (Xiao Decl. Exh. 10 at 1.)

That same day, Krzanich explained in an interview that Intel had been working with all of the Company's industry partners, including operating system vendors and OEMs, to patch and resolve the problem. (CCAC ¶ 109.) He assured the public that "we believe we have the right fixes in place. We've been testing those fixes and making sure that we understand how to implement those." (*Id*. (internal quotation marks omitted).) Intel's stock price fell another 2%, erasing additional billions of dollars in market capitalization. (*Id*. ¶ 113.)

On January 4, 2018, Intel issued a press release, announcing that the Company had developed and was rapidly issuing updates for all types of Intel-based computers systems that render those systems immune from both the Spectre and Meltdown exploits. (*Id*. ¶ 114.) Intel further represented that it "continues to believe that the performance impact of these updates is highly workload-dependent and, for the average computer user, should not be significant and will be mitigated over time." (*Id*. (internal quotation marks omitted).)

On January 8, 2018, Krzanich acknowledged that fixes for Spectre and Meltdown would slow the performance of processors and that the problem may be more pervasive than defendants originally represented. (*Id*. ¶ 115.) Intel's customers and independent experts corroborated the significant performance degradation the patches caused. (*Id*. ¶¶ 114, 117, 120.) For example, on January 9, 2018, Microsoft released data showing that the patches may "significant[ly]" slow

down the performance of certain services and some personal computers. (*Id*. ¶ 117.) On this news, Intel's stock price declined another 2.5%, a market capitalization loss of $5.2 billion. (*Id*. ¶ 118.) A prominent software engineer characterized Intel's patches as "COMPLETE AND UTTER GARGBAGE." (*Id*. ¶ 124 (emphasis in original).) Intel's stock price fell another 2.6% on January 10, 2018, a market capitalization loss of $5.2 billion. (*Id*. at ¶ 122.)

Plaintiff alleges that Spectre and Meltdown exploit fundamental design defects in Intel's processors. The defects can only be partially fixed, and at substantial cost to performance. The only effective long-term fix for Spectre is entirely redesigning the chips; it cannot be mitigated by installing a patch of software code on a computer's operating system. (*Id*. ¶¶ 59, 60.) As one researcher put it, the threat from Spectre is "going to live with us for decades." (*Id*. ¶ 60 (internal quotation marks omitted).) The Meltdown flaw can be mitigated with a patch, but the patch significantly impacts and slows down computer performance. (*Id*. ¶ 62.) One such fix, known as "Kernel Page Table Isolation," reduces performance by up to 30 percent. (*Id*.)

In the aftermath, Intel continued to struggle with Meltdown and Spectre. A former Intel leader explained that there were 135 or more malware items meant to exploit Spectre, Meltdown, and issues with the patches. (*Id*. ¶ 125.) In May 2018, Intel likewise confirmed reports of eight additional threats from the next generation of Spectre, each of which requires its own patches. (*Id*. ¶ 127.) Intel disclosed that patches for the four "high-risk" threats would be unavailable until at least August 2018. (*Id*. (internal quotation marks omitted).)

C. ALLEGEDLY FALSE AND MISLEADING STATEMENTS AND OMISSIONS

Plaintiff alleges that Intel continued to promote the security and performance of its processors to investors in various contexts throughout the Class Period without disclosing Spectre and Meltdown. Specifically, plaintiff alleges myriad false and misleading statements in relation to the security and performance of Intel's processors. As pled in the CCAC, plaintiff's securities fraud claim centers on seven categories of statements as set forth in Appendix A hereto. Each category addresses a specific context in which statements were made.[7]

[7] The statements in Appendix A are copied verbatim from the CCAC, and all emphases in defendants' allegedly false and misleading statements therein and in this Order are originally

II. LEGAL STANDARD

Defendants bring this motion pursuant to Federal Rules of Civil Procedure 8(a), 9(b), and 12(b)(6). In general, Rule 8(a) requires that a complaint contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). A defendant may move to dismiss a complaint for failing to state a claim upon which relief can be granted under Rule 12(b)(6). "Dismissal can be based on the lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988). All allegations of material fact are taken as true and construed in the light most favorable to the plaintiff. *Johnson v. Lucent Techs. Inc.*, 653 F.3d 1000, 1010 (9th Cir. 2011). To survive a motion to dismiss, "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). That requirement is met "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id*.

Furthermore, claims for fraud must meet the particularity requirements of Rule 9(b), including "an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations." *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007) (citing Rule 9(b)) (internal quotation marks omitted). However, private securities fraud complaints are subject to the "more exacting pleading requirements" of the PSLRA, which requires that the complaint plead both falsity and scienter with particularity. *Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 990 (9th Cir. 2009). "[T]he inference of scienter must be more than merely 'reasonable' or 'permissible'—it must be cogent and compelling, thus strong in light of other explanations" and a court "must consider plausible, nonculpable explanations for the defendant's conduct[.]" *See Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 324 (2007).

---

supplied by the CCAC unless otherwise noted. The portions of the broader statements emphasized in italics and bold typeface are presumably meant to indicate a false or misleading statement.

III. THRESHOLD ISSUES

Defendants present nineteen documents in support of their motion to dismiss. For each, they request that the Court take judicial notice thereof, pursuant to Federal Rule of Evidence 201, or incorporate the document by reference.[8] Specifically, defendants request that the Court take judicial notice of Exhibits 1–3, 6–8, and 13–16, and treat as incorporated by reference Exhibits 10–12. As for Exhibits 4–5, 9, and 17–19, defendants request that the Court take judicial notice of them *and* treat them as incorporated by reference. (*See* Dkt. No. 73.) Plaintiff challenges each of these requests, relying principally on *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988 (9th Cir. 2018). (*See* Dkt. No. 70.) Importantly, consideration of this issue informs the Court's evaluation of the sufficiency of the CCAC.

In *Khoja*, the Ninth Circuit considered whether the district court had overused the

[8] The nineteen documents include:

(1) Microsoft's Security Guide (Xiao Decl. Exh. 1, Dkt. No. 67-2);
(2) Intel's Product Security Center Advisories (*id*. Exh. 2, Dkt. No. 67-3 ("Security Advisories"));
(3) "Announcing Project Zero" Google Blog Post (*id*. Exh. 3, Dkt. No. 67-4);
(4) "Researchers Discover Two Major Flaws in the World's Computers" *New York Times* Article (*id*. Exh. 4 ("*New York Times Article*"), Dkt. No. 67-5);
(5) "Keeping Spectre Secret" *The Verge* Article (*id*. Exh. 5 ("*The Verge* Article"), Dkt. No. 67-6);
(6) The CERT Guide to Coordinated Vulnerability Disclosure (*id*. Exh. 6, Dkt. No. 67-7);
(7) Intel's Vulnerability Handling Guidelines (*id*. Exh. 7, Dkt. No. 67-8);
(8) Intel's Security Advisory 00077 (*id*. Exh. 8, Dkt. No. 67-9);
(9) Intel's Form 10-K (2016);
(10) "Intel Responds to Security Research Findings" Intel Newsroom Article (*id*. Exh. 10, Dkt. No. 67-11);
(11) "CERT: Only way to fix Meltdown and Spectre vulnerabilities is to replace CPU" *VentureBeat* Article (*id*. Exh. 11, Dkt. No. 67-12);
(12) Transcript of January 3, 2018 Intel Investor Call (*id*. Exh. 12, Dkt. No. 67-13);
(13) Intel's Form 8-K (Q4 2017) (*id*. Exh. 13, Dkt. No. 67-14);
(14) Intel's Historical Stock Prices (*id*. Exh. 14, Dkt. No. 67-15);
(15) "Intel is Top-Performing Dow Stock in Q1" *24/7 Wall St.* Article (*id*. Exh. 15, Dkt. No. 67-16);
(16) Intel's Form 8-K (Q1 2018) (*id*. Exh. 16, Dkt. No. 67-17);
(17) Intel Product Webpages (*id*. Exh. 17 ("Product Webpages"), Dkt. No. 67-18);
(18) Intel's Form 10-Q (Q3 2017) (*id*. Exh. 18, Dkt. No. 67-19); and
(19) US-Cert Guidelines (*id*. Exh. 19, Dkt. No. 67-20).

incorporation by reference and judicial notice doctrines in a securities case to dismiss "what would otherwise constitute adequately stated claims at the pleading stage." *Khoja*, 899 F.3d at 998. The court cautioned that if defendants are permitted to present their own version of the facts at the pleading stage, and district courts accept such facts as true, it would be "near impossible" for even the most aggrieved plaintiff to demonstrate a plausible claim for relief. *Id*. at 999.

That said, incorporation by reference is a judicial doctrine that prevents plaintiffs from selecting only portions of documents that support their claims, while omitting portions of those very documents that weaken or extinguish their claims. *Id*. at 1002. Application of the doctrine in a particular case can be tricky. Generally, a court may assume an incorporated document's contents are true for purposes of a motion to dismiss under Rule 12(b)(6). *Id*. at 1003. It is improper, however, to assume the truth of everything in an incorporated document for the sole purpose of disputing facts stated in a well-pleaded complaint. *Id*. A defendant may seek to incorporate a document into the complaint if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim. *Id*. at 1002. The mere mention of the existence of a document, however, is insufficient to incorporate the contents of a document. *Id*. The Ninth Circuit emphasized that the doctrine must not be used as a tool by defendants to "short-circuit the resolution of a well-pleaded claim." *Id*.

Judicial notice, on the other hand, is appropriate for "adjudicative fact[s]" that are "not subject to reasonable dispute." Fed. R. Evid. 201(a), (b). The Ninth Circuit has cautioned that simply because a document is susceptible to judicial notice "does not mean that every assertion of fact within that document is judicially noticeable for its truth." *Khoja*, 899 F.3d at 999.

The Court concludes that it may properly take judicial notice of Exhibit 2, not for the truth of its content, but to "indicate what was in the public realm at the time." *Von Saher v. Norton Simon Museum of Art at Pasadena*, 592 F.3d 954, 960 (2010) (internal quotation marks omitted); *Gerritsen v. Warner Bros. Entm't Inc.*, 112 F. Supp. 3d 1011, 1028 (C.D. Cal. 2015) ("The cases in which courts take judicial notice of newspaper articles and press releases . . . are limited to a narrow set of circumstances . . . e.g., in securities cases *for the purpose of showing that particular information was available to the stock market*.") (emphasis supplied); *see also, e.g., Heliotrope*

Gen., Inc. v. Ford Motor Co., 189 F.3d 971, 981 n.18 (9th Cir. 1999) (taking judicial notice "that the *market was aware of the information* contained in news articles submitted by the defendants") (emphasis supplied). This exhibit further meets the standard for admissibility set forth in Federal Rule of Evidence 201(b).

With respect to use of the incorporation by reference doctrine, the Court finds that plaintiff references Exhibits 4 and 10 substantively. Thus, plaintiff does more than merely mention both Exhibit 4 as it is cited in two paragraphs of the CCAC, (*see id*. ¶¶ 60, 63), and Exhibit 10 as it is quoted or referenced in three paragraphs therein, (*see* ¶¶ 107, 181, 182). Accordingly, both are incorporated by reference.[9] As for Exhibit 5, the Court finds that it is not incorporated by reference as plaintiff cites the article *once*, in a footnote, in support of just three sentences of the CCAC. *See id*. ¶ 69 n.20 & accompanying text; *see also Khoja*, 899 F.3d at 1003 ("For 'extensively' to mean anything under [*United States v. Ritchie*, 342 F.3d 903 (9th Cir. 2003)], it should, ordinarily at least, mean more than once."). Nor does the article form the basis of any claim in the CCAC. *See Khoja*, 899 F.3d at 1002. However, the Court may properly take judicial notice of Exhibit 5, not for the truth of its content, but "for the purpose of showing that particular information was available to the stock market." *Gerritsen*, 112 F. Supp. 3d at 1028.

As for Amended Exhibit 9, the 2016 Form 10-K, it is not mentioned in the CCAC, nor do plaintiff's claims necessarily depend on it, thus incorporation by reference is not appropriate. However, the Court may properly take judicial notice of Amended Exhibit 9 since SEC filings are routinely subject to judicial notice. *See Dreiling v. Am. Exp. Co.*, 458 F.3d 942, 946 n.2 (9th Cir. 2006). As for Exhibit 17, the Court finds that it is incorporated by reference since plaintiff quotes the webpages extensively and relies on them in support of its claims. (*See* CCAC ¶¶ 148, 149, 152, 153.)[10]

[9] In any event, the Court notes that it can take judicial notice of the article at Exhibit 4, not for the truth of its content but "for the purpose of showing that particular information was available to the stock market." *Gerritsen*, 112 F. Supp. 3d at 1028.

[10] Accordingly, the Court need not address defendants' request that the Court take judicial notice of this exhibit. *See Morris v. Mott's LLP*, No. SACV 18-01799 AG (ADSx), 2019 WL 948750, at *1 (C.D. Cal. Feb. 26, 2019) ("The Court need not take judicial notice of the label

The remaining documents, namely Exhibits 1, 3, 6–8, 11–16, and 18–19, were not relevant to the Court's analysis. Defendants' requests as to these exhibits are thus **DENIED AS MOOT**.

IV. COUNT I: SECTION 10(b) OF THE EXCHANGE ACT AND RULE 10-b5

A. LEGAL FRAMEWORK

Section 10(b) of the Exchange Act makes it unlawful for any person to "use or employ, in connection with the purchase or sale of any security . . . any manipulative or deceptive device or contrivance in contravention of such rules and regulations as the Commission may prescribe as necessary or appropriate in the public interest or for the protection of investors." 15 U.S.C. § 78j(b). SEC Rule 10b–5 implements this provision by making it unlawful to "make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading[.]" 17 C.F.R. § 240.10b–5(b). Similarly, under the Exchange Act, any person who "directly or indirectly, controls any person liable under any provision of [the Exchange Act] or any rule or regulation thereunder shall also be liable jointly and severally with and to the same extent as such controlled person to any person to whom such controlled person is liable . . . ." 15 U.S.C. § 78t(a).

In 1995, Congress enacted the PSLRA, which includes "[e]xacting pleading requirements," as a check against abusive litigation by private parties. *Tellabs*, 551 U.S. at 313.[11] Heightened pleading is one of the control measures Congress included to advance "the PSLRA's twin goals: to curb frivolous, lawyer-driven litigation, while preserving investors' ability to recover on meritorious claims." *Id.* at 322.

To state a claim under Section 10(b), a plaintiff "must show that the defendant made a

---

because it's incorporated by reference into Plaintiff's complaint.").

[11] Members of the House and Senate "observed that plaintiffs routinely were filing lawsuits against issuers of securities and others whenever there [was] a significant change in an issuer's stock price, without regard to any underlying culpability of the issuer, and with only faint hope that the discovery process might lead eventually to some plausible cause of action[.]" *In re Silicon Graphics Inc. Sec. Litig.*, 183 F.3d 970, 978 (9th Cir. 1999), *as amended* (Aug. 4, 1999) (internal quotation marks omitted) (alterations in original).

statement that was '*misleading* as to a *material* fact.'" *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 38 (2011) (quoting *Basic Inc. v. Levinson*, 485 U.S. 224, 238 (1988)) (emphases in original). Under the PSLRA's heightened pleading requirement, to state a Section 10(b) claim, plaintiffs must allege facts sufficient to establish: (i) that the defendant made a material misrepresentation or omission of fact, (ii) with scienter; (iii) a connection between the misrepresentation or omission and the purchase or sale of a security; (iv) reliance on the misrepresentation or omission; (v) loss causation; and (vi) economic loss. *Loos v. Immersion Corp.*, 762 F.3d 880, 886–87 (9th Cir. 2014) (citing *Dura Pharm., Inc. v. Broudo*, 544 U.S. 336, 341–42 (2005)). Under Rule 9(b), claims alleging fraud are subject to a heightened pleading requirement, which requires that a party "state with particularity the circumstances constituting fraud or mistake." Fed. R. Civ. P. 9(b); *see supra* at 8. With respect to the scienter requirement, the Court must view the allegations as a whole and determine whether plaintiff has raised an inference of scienter that is "cogent and compelling, thus strong in light of other explanations," to satisfy the PSLRA standard. *S. Ferry LP, No. 2 v. Killinger*, 542 F.3d 776, 784 (9th Cir. 2008) (internal quotation marks omitted). When assessing the allegations holistically, the Court views circumstances that are probative of scienter with a "practical and common-sense perspective." *Id.*

Here, defendants challenge the sufficiency of the first two elements: material misrepresentation or omission and scienter. Each element is discussed below.

B. DISCUSSION

1. First Relevant Element: Material Misrepresentation or Omission

a. Legal Standard

"Materially misleading statements or omissions by a defendant constitute the primary element of a section 10(b) and rule 10b-5 cause of action." *In re Immune Response Sec. Litig.*, 375 F. Supp. 2d 983, 1017 (S.D. Cal. 2005) (quoting *Marksman Partners, L.P. v. Chantal Pharm. Corp.*, 927 F. Supp. 1297, 1305 (C.D. Cal. 1996)). To plead this element, a complaint must "identify[] the statements at issue and set[] forth what is false or misleading about the statement and why the statements were false or misleading at the time they were made." *In re Rigel Pharm, Inc. Sec. Litig.*, 697 F.3d 869, 876 (9th Cir. 2012).

With regard to falsity, that element is adequately alleged "when a plaintiff points to [the] defendant's statements that directly contradict what the defendant knew at that time." *Khoja*, 899 F.3d at 1008 (citing *In re Atossa Genetics Inc. Sec. Litig.*, 868 F.3d 784, 794–96 (9th Cir. 2017)). To plead falsity under the PSLRA, a plaintiff must "specify each statement alleged to have been misleading" and the "reasons why the statement is misleading[.]" 15 U.S.C. § 78u-4(b)(1)(B); *Zucco*, 552 F.3d at 990–91. A statement is misleading "if it would give a reasonable investor the impression of a state of affairs that differs in a material way from the one that actually exists." *Retail Wholesale & Dep't Store Union Local 338 Ret. Fund v. Hewlett-Packard Co.*, 845 F.3d 1268, 1275 (9th Cir. 2017) (internal quotation marks omitted). To be misleading, a statement must be "capable of objective verification." *Or. Pub. Emps. Ret. Fund v. Apollo Grp. Inc.*, 774 F.3d 598, 606 (9th Cir. 2014). For example, "puffing"—expressing an opinion rather than a knowing false statement of fact—is not misleading. *Id.*; *see also Lloyd v. CVB Fin. Corp.*, 811 F.3d 1200, 1206–07 (9th Cir. 2016); *In re Cutera Sec. Litig.*, 610 F.3d 1103, 1111 (9th Cir. 2010). Qualitative buzzwords such as "good," "well-regarded," or other "vague statements of optimism" cannot form the basis of a false or misleading statement. *Apollo*, 774 F.3d at 606 (citing *Cutera*, 610 F.3d at 1111 ("When valuing corporations, . . . investors do not rely on vague statements of optimism like 'good,' 'well-regarded,' or other feel good monikers. This mildly optimistic, subjective assessment hardly amounts to a securities violation.")). Indeed, "professional investors, and most amateur investors as well, know how to devalue the optimism of corporate executives[.]" *In re VeriFone Sec. Litig.*, 784 F. Supp. 1471, 1481 (N.D. Cal. 1992), *aff'd sub nom.*, 11 F.3d 865 (9th Cir. 1993).

Even if a statement is not false, it may be misleading if it omits material information. *Khoja*, 899 F.3d at 1008–09 (citing *In re NVIDIA Corp. Sec. Litig.*, 768 F.3d 1046, 1054 (9th Cir. 2014)). "[A]n omission is material 'when there is a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the total mix of information available.'" *Markette v. XOMA Corp.*, No. 15-cv-03425-HSG, 2017 WL 4310759, at *7 (N.D. Cal. Sept. 28, 2017) (quoting *Matrixx*, 563 U.S. at 38). But omissions are actionable only where they "make the actual statements misleading": it is not

sufficient that an investor "consider the omitted information significant." *Id*. (internal quotation marks omitted).

Whether a plaintiff alleges an omission or misstatement, an actionable representation must be material. *See Cutera*, 610 F.3d at 1108 ("Central to a 10b–5 claim is the requirement that a misrepresentation or omission of fact must be material."). For purposes of a 10b-5 claim, "a misrepresentation or omission is material if there is a substantial likelihood that a reasonable investor would have acted differently if the misrepresentation had not been made or the truth had been disclosed." *Livid Holdings Ltd. v. Salomon Smith Barney, Inc.*, 416 F.3d 940, 946 (9th Cir. 2005).

b. Analysis

Whereas the CCAC points generally to the numerous allegedly false or misleading statements detailed in Appendix A, the parties' briefing has organized the statements into two broad categories, namely statements about (i) chip security and (ii) chip performance. (*See, e.g.*, Opposition to Defendants' Motion to Dismiss Consolidated Complaint ("Opp.") at 11, Dkt. No. 69.) For simplicity, the Court adopts those categories herein and addresses them below.

i. Chip Security

The majority of the allegedly false and misleading statements plaintiff identifies pertaining to chip security are nonactionable, as they constitute mere puffery or are otherwise non-verifiable "vague statements of optimism." *Cutera*, 610 F.3d at 1111. Such chip-security statements were marketing statements to the effect that Intel's products offer security-related features that, for example:

- are "***optimized particularly for data protection***," (CCAC ¶ 88);
- ***"add[] a critical layer of protection*** to make password logons, browsing, and online payments ***safe and simple***," and are "***rock-solid***," (*id*. ¶ 132; *see also id*. ¶ 136);
- provide "***[h]ardware-level technologies that strengthen the protection of enabled security software***," and "***[h]ardware-based security***," (*id*. ¶ 138; *see also id*. ¶ 144 ("***count on hardware-based security***"));
- provide a "***robust multifactor verification solution that is protected in hardware, reducing exposure to software-level attacks***," (*id*. ¶ 140);

- provide "***[h]ardware-[e]nhanced [s]ecurity***," (*id*.; *see also id*. ¶ 148 ("[e]xperience . . . ***hardware-enhanced security***"));
- provide "***optimal data security***," (*id*. ¶ 142);
- "***[i]mprove [s]ecurity***," (*id*. ¶ 144);
- "***provide a critical foundation for secure IT***," (*id*. ¶ 146);
- provide "***[s]ecurity you can trust***" and "a ***more secure operating environment***," allowing computer users to have "peace of mind," (*id*. ¶ 152);
- provide "***[p]rotection capabilities***," (*id*.);
- make it "***easy to secure all your data***," (*id*.);
- provide "***advanced security features***," (*id*. ¶ 157); and
- "***have the ability to protect against identity breaches***" and "***[p]rotect[] the good people from the bad people***," (*id*. ¶ 167).

The Court finds these constitute vague positive statements which are immaterial as a matter of law. *See, e.g.*, *Kelly v. Elec. Arts, Inc.*, No. 13-cv-05837-SI, 2015 WL 1967233, at *7–8 (N.D. Cal. Apr. 30, 2015) (holding that the term "de-risk," like the word "improved," "signifies making a product better or safer, and is a statement of corporate optimism and a vague assessment of past results"); *City of Roseville Emps.' Ret. Sys. v. Sterling Fin. Corp.*, 47 F. Supp. 3d 1205, 1220 (E.D. Wash. 2014) (statement that company was maintaining "safe and sound banking practices" was "too general and would not cause investors to rely upon it"); *In re Cisco Sys. Inc. Sec. Litig.*, No. C 11-1568 SBA, 2013 WL 1402788, at *13 (N.D. Cal. Mar. 29, 2013) (statement that company had a "strong foundation" was found to be "corporate puffery on which no reasonable investor would rely") (internal quotation marks omitted); *In re Splash Tech. Holdings., Inc. Sec. Litig.*, 160 F. Supp. 2d 1059, 1077 (N.D. Cal. 2001) (holding that phrases such as "strong," "better than expected," "robust," "well positioned," "solid," and "improved," when used to describe demand, results, and growth strategy, were not actionable as material misrepresentations); *see also, e.g.*, *Shemian v. Research in Motion Ltd.*, No. 11 Civ. 4068(RJS), 2013 WL 1285779, at *20 (S.D.N.Y. Mar. 29, 2013) (defendants' statements regarding "advanced security features" and "very powerful hardware" did not give rise to any duty to disclose), *aff'd*, 570 F. App'x 32 (2d Cir. 2014).

Because the Court cannot quantify these statements for their truth or falsity, they are not actionable.

Those statements that may be "capable of objective verification," however, do not fare any better. *Apollo*, 774 F.3d at 606. Thus: plaintiff first argues that defendants' statement that Intel's processors were "***vulnerability-resistant***," (CCAC ¶ 150), was false and misleading in light of the Spectre and Meltdown vulnerabilities. (*See* Opp. at 2–3, 7–8.) Plaintiff does not persuade. Just as "water-resistant" does not mean "water-proof," reasonable investors understand that a "vulnerability-resistant" product is not guaranteed to be immune from any and all security issues. *See, e.g.*, *Searls v. Glasser*, 64 F.3d 1061, 1066 (7th Cir. 1995) (distinguishing between the phrases "recession-resistant" and "recession-proof" and concluding that the former is "simply too vague to constitute a material statement of fact").

Next, plaintiff's reliance on the statement that the security features of Intel's Xeon chips "***address[ed] the numerous, increasing, and evolving security threats***" is similarly unavailing. (CCAC ¶ 146; *see also* Opp. at 2–3.) The CCAC pleads no facts showing this statement to be untrue, *i.e.*, that the Xeon chip's security features did not actually address numerous security threats. Moreover, a statement that a feature merely "addresses" a category of threats which are "increasing" and "evolving" is distinguishable from a statement that the feature will *categorically eliminate* any threat. Absent specific allegations that this and the prior statement were false, the CCAC "falls short of the PSLRA's exacting standard." *See In re Nimble Storage, Inc. Sec. Litig.*, No. 17-17232, 2019 WL 1212819, at *1 (9th Cir. Mar. 14, 2019).[12]

Plaintiff's stronger argument is that defendants misled investors by stating that (i) Intel's X-series processors "***protect[] internet and email content***," (CCAC ¶ 134), (ii) its Xeon Scalable

[12] The Court recognizes that statements which are not false may still be misleading if they omit material information. *See Khoja*, 899 F.3d at 1008–09. However, given the total mix of information, as described below, reasonable investors would not be misled regarding the potential for security threats by defendants' statements that Intel's processors were "***vulnerability-resistant***" and that the security features of Intel's Xeon chips "***address[ed] the numerous, increasing, and evolving security threats***." Thus, defendants' omission of Spectre and Meltdown was not material given the context in which the statements were made, and the Court need not address the other materiality arguments advanced by defendants. *See* MTD at 15–16.

processors "ensur[e] an effective IT security platform," (*id*. ¶ 146; *see also* Tr. 34:7–22, 34:24–35:3), and (iii) its Pentium and Celeron processors "help[] keep your ***device safe, blocking dangerous programs***," (CCAC ¶ 152). The words "protect," "ensure," and "block" are undoubtedly more definitive than the words "resistant" and "address." However, plaintiff must allege falsity in light of "specific 'contemporaneous statements or conditions' that demonstrate the intentional or deliberately reckless false or misleading nature of the statements when made." *Ronconi v. Larkin*, 253 F.3d 423, 432 (9th Cir. 2001).[13] Courts evaluate defendants' alleged false statements in the context in which they were made, specifically in regard to contemporaneous qualifying or clarifying language. *In re Syntex Corp. Sec. Litig.*, 95 F.3d 922, 929 (9th Cir. 1996) (holding statements non-actionable where the "statement in full and in context at the time" acknowledged uncertainty). The industry also provides context insofar as the computer industry "involves the situation where shareholders invest in an industry that is laden with risk." *Id*. at 933. Critically, plaintiff must "demonstrate that a particular statement, when *read in light of all the information then available* to the market . . . conveyed a false or misleading impression." *In re Convergent Techs. Sec. Litig.*, 948 F.2d 507, 512 (9th Cir. 1991), *as amended on denial of reh'g* (Dec. 6, 1991) (emphasis supplied); *see also, e.g., Padnes v. Scios Nova Inc.*, No. C 95-1693 MHP, 1996 WL 539711, at *9 (N.D. Cal. Sept. 18, 1996) (granting a motion to dismiss where publicly available information contradicted the alleged false public statement when it was made).

Here, plaintiff contends that defendants "spoke directly about security" without disclosing Spectre or Meltdown and that a Section 10(b) claim can be based on failure to provide context. (Opp. at 9.) However, the relevant context undermines plaintiff's allegations of falsity. Specifically, that context includes not only the words and sentences surrounding the challenged phrases, shown above, but also: (i) the marketing setting in which the statements were made;[14]

---

[13] Plaintiff here concedes that the Court must consider the context in which the statements were made. *See* Opp. at 15.

[14] *See Bien v. LifeLock, Inc.*, No. CV-014-00416-PHX-SRB, 2015 WL 12819154, at *9 (D. Ariz. July 21, 2015) (finding that plaintiffs failed to allege that product advertisements met the "in connection with" the purchase or sale of securities element of the Exchange Act where complaint "fail[ed] to provide sufficient factual allegations demonstrating that reasonable investors would base their investment decisions on the advertisements in this case"); *see also Di*

(ii) Intel's disclaimer that "[n]o computer system can be absolutely secure[,]" (Product Webpages at ECF p. 5); (iii) other statements Intel made on its website about various other security vulnerabilities identified, including any fixes or workarounds, (*see generally* Security Advisories); (iv) the risk warnings about security vulnerabilities in Intel's SEC filings (*see* 2016 Form 10-K at 20 (conveying that Intel's products "are a frequent target" of hackers and that "[f]rom time to time" intrusions occur));[15] (v) the inherently risky nature of the computer industry; (vi) Intel's then-ongoing efforts to develop a solution to the Spectre and Meltdown vulnerabilities, (*see* CCAC ¶ 110); (vii) the industry practice of "keep[ing] the news [of security vulnerabilities] from the public so hackers [cannot] take advantage of [such] flaws before they [a]re fixed," (*see New York Times* Article at 2; *see also The Verge* Article at 2); and (viii) plaintiff's failure to allege any reported hacks resulting from the Spectre and Meltdown vulnerabilities. Viewed against this backdrop, these three particular statements on which plaintiff relies did not create a false impression regarding the security of Intel's processors, nor, given this context, would they mislead reasonable investors regarding the potential for security threats.

///

///

Donato v. Insys Therapeutics Inc., No. CV-16-00302-PHX-NVW, 2017 WL 3268797, at *16 (D. Ariz. Aug. 1, 2017) (explaining that "[t]he kinds of statements courts have found to satisfy the 'in connection with' requirement are typically documents directly targeted to investors or the investment community," namely audit reports that would be included in SEC filings, annual and quarterly reports, press releases, conference calls, and account statements and newsletters sent directly to investors). While Intel's product statements appear to be a far cry from the typical statements upon which an investor would presumably rely, the Court agrees with plaintiff that "there is no rule that only market-related documents, such as regulatory filings, public presentations, or press releases can contain actionable misstatements under Section 10(b)." Opp. at 10 (internal quotation marks omitted). However, the CCAC does not allege that the product statements were directly targeted to investors or the investment community. That defendants may have "directed investors to visit the Company's website for [n]ews and information about Intel® products and technologies" is insufficient in this regard. CCAC ¶ 77 (internal quotation marks omitted) (alteration in original).

[15] Plaintiff's argument that "Intel's 'risk warnings' themselves were misleading in that they discussed the ***potential*** for security vulnerabilities that were ***already occurring***," (*see* Opp. at 12 (emphases in original)), overlooks that Intel's warnings conveyed that Intel's products "*are* a frequent target" of hackers and that "[f]rom *time to time*" intrusions occur. 2016 Form 10-K at 20 (emphases supplied).

ii. Chip Performance

As with the chip-security statements, many of the allegedly false and misleading statements plaintiff identifies pertaining to chip performance are nonactionable, as they constitute mere puffery or non-verifiable vague statements of optimism. For example, defendants claimed Intel's platforms:

- "improve[] performance by creating faster multitasking ***with optimal data security***," (CCAC ¶ 142);
- "***[i]mprove [s]ecurity***," namely by providing "***hardware-enhanced security to protect data and system operations without compromising performance***," (*id*. ¶ 144);
- "***optimize interconnectivity with a focus on speed without compromising data security***," (*id*.);
- "***protect data and system operations without compromising performance***[,]" (*id*.); and
- provide "***strong security without compromising performance or impacting your experience***[,]" (*id*. ¶ 152);

Defendants also promoted the following processor features:

- "**[u]nprecedented [p]ower and [r]esponsiveness**" and "***a big jump in performance***," (*id*. ¶ 132; *see also id*. ¶ 136);
- "***[e]xceptional platform performance***," (*id*. ¶ 138);
- "***[e]ssential performance***" and "***professional-grade compute performance***," (*id*. ¶ 148);
- "***hardware-enhanced performance***," (*id*.);
- "***significant performance improvement***," (*id*. ¶ 154); and
- "***outstanding performance***," (*id*. ¶ 160).

Here, again, the Court finds these types of statements to be vague and immaterial as a matter of law. *See, e.g.*, *Lomingkit v. Apollo Educ. Grp. Inc.*, 275 F. Supp. 3d 1139, 1152 n.6 (D. Ariz. 2017) (finding the term "significant enhancement" to be corporate puffery); *In re Calpine Corp.*, 288 F. Supp. 2d 1054, 1088 (N.D. Cal. 2003) (holding that words such as "strong," "healthy," and "solid" could not form a basis for the plaintiffs' Exchange Act claims); *Splash*, 160 F. Supp. 2d at 1077 (finding statements using the words "strong," "robust," "well positioned," "solid" and "improved" to be "vague and nonactionable"); *see also, e.g., In re Stratasys Ltd. S'holder Sec.*

Litig., 864 F.3d 879, 882 (8th Cir. 2017) (company's statements that its printers offered "unmatched speed, reliability, quality, and connectivity" were "vague and nonverifiable").

Further, plaintiff has not alleged that any of the facts contained within any of the other more specific statements were, in fact, inaccurate. Defendants stated, for example, that:

- Intel's Pentium and Celeron processors have "***30% more processor performance*** . . . than the previous generation platform," (CCAC ¶ 152);
- Intel's Coffee Lake family of processors has "***up to 50% better performance than the competition on top-game titles***[,]" (*id*. ¶ 155);
- Intel's Xeon Scalable Processors have a "***1.73X average performance boost*** vs. the previous generation across key industry-standard workloads," and are "optimized to deliver 2.2X higher deep learning training and up to ***2.4X higher inference performance*** compared to the prior generation[,]" (*id*. ¶ 157);
- Intel's Xeon Scalable Processors "outperform[] [other x86 offerings] on throughputs, kind of benchmarks by 34%, by 18% on performance per watt benchmarks and by over 50% on performance per core," (*id*. ¶ 97; *see also id*. ¶ 159); and
- "***[I]f you do a like-by-like performance, from the first product in 14, Broadwell, for example, to the eighth generation Intel device, we've seen an over 30% improvement in the performance of the devices. And that's just a testament to how much intra-node benefit there is.***" (*Id*. ¶ 165 (alteration in original).)

While these claims presumably could be verified, plaintiff fails to plead facts showing the statements were false.[16] To the extent the statements compare newer to older products and to competitors' products, the CCAC expressly acknowledges that "Spectre and Meltdown affect nearly every processor Intel has released since 1995" in addition to competitors' processors. (*Id*. ¶ 3; *see also id*. ¶ 56.) Thus, the notion that the discovery of the vulnerabilities rendered the comparisons inaccurate is unavailing. Absent specific allegations that the statements were false, the CCAC fails to meet the PSLRA's demanding standard.[17]

---

[16] In its opposition and at oral argument, plaintiff cited a footnote, now on Intel's website, stating that the solutions for Spectre and Meltdown made the cited performance metrics "inapplicable to your device or system." Opp. at 11 (citing CCAC ¶ 129); Tr. at 23:15–22. This disclaimer, as plaintiff notes, was added after the Class Period ended and after solutions were deployed. It falls short of showing that any of defendants' statements were false *during the Class Period*.

[17] Again, given the total mix of information, as described herein, reasonable investors would not be misled regarding the potential for security threats by defendants' verifiable chip-performance statements. *See supra at* 18–19. Defendants' omission of Spectre and Meltdown

In short, the CCAC does not allege facts to establish that defendants made any materially false or misleading statements.[18]

2. Second Relevant Element: Scienter

Because the Court finds that plaintiff has failed to allege any actionable statements or omissions under Section 10(b) and Rule 10b-5, the Court need not address whether plaintiff adequately alleged scienter, despite the Court's concerns regarding the nature and timing of Krzanich's sale of Intel shares. *See Reese v. BP Exploration (Alasksa) Inc.*, 643 F.3d 681, 694 (9th Cir. 2011); *see also In re Connetics Corp. Sec. Litig.*, 542 F. Supp. 2d 996, 1012–13 (N.D. Cal. 2008).

V. COUNT II: SECTION 20(a) OF THE EXCHANGE ACT

Under Section 20(a), "a defendant employee of a corporation who has violated the securities laws will be jointly and severally liable to the plaintiff, as long as the plaintiff demonstrates a primary violation of federal securities law and that the defendant exercised actual

---

was therefore not material given the specific context at issue, and the Court need not address the other materiality arguments advanced by defendants. *See* MTD at 15–16.

Given the Court's conclusion that none of defendants' statements were materially misleading, plaintiff's theory that defendants had a "duty to disclose Spectre and Meltdown to make their statements about the security and performance features of the Company's processors not misleading" fails. Opp. at 8; *see also Matrixx*, 563 U.S. at 44 ("Disclosure is required . . . only when necessary to make . . . statements made, in light of the circumstances under which they were made, not misleading.") (internal quotation marks omitted) (alteration in original). Plaintiff's separate argument that Krzanich's trading of Intel stock gave rise to a duty to disclose is foreclosed by settled law. *See* Opp. at 9–10; *see also Anderson v. Abbott Labs.*, 140 F. Supp. 2d 894, 909–10 (N.D. Ill. 2001) ("[T]his is not an insider trading case. An insider's duty to disclose is not transferable to the securities fraud claim against the corporate defendant or the individual defendants.") (internal quotation marks omitted); *see also In re Seagate Tech. II Sec. Litig.*, 843 F. Supp. 1341, 1369–70 (N.D. Cal. 1994) (rejecting the plaintiffs' efforts to establish a "duty to disclose based on the alleged insider trading of two of the individual defendants").

[18] Plaintiff's contention that defendants are raising a "truth on the market" defense, (Opp. at 12), fails to persuade. Such a defense applies where "a defendant's failure to disclose material information may be excused where the information was made credibly available to the market by other sources." *Nguyen v. Radient Pharm. Corp.*, No. SA CV 11-0406 DOC (MLGx), 2011 WL 5041959, at *6 (C.D. Cal. Oct. 20, 2011) (citing *In re Amgen, Inc. Sec. Litig.*, 544 F. Supp. 2d 1009, 1025 (C.D. Cal. 2008)). Here, defendants argue that they disclosed all required information, not that they failed to make required disclosures but should be excused because other sources have already made the same information available. *See Chang v. Accelerate Diagnostics, Inc.*, No. CV-15-00504-PHX-SPL, 2016 WL 3640023, at *5 (D. Ariz. Jan. 28, 2016) ("Defendants assert that the statements themselves, read in context, are simply not false or misleading. . . . This is not a truth-on-the-market defense.") (internal quotation marks omitted).

power or control over the primary violator." *Zucco*, 552 F.3d at 990 (internal quotation marks omitted).

In light of the above with regard to plaintiff's Section 10(b) claim, plaintiff's Section 20(a) claim against the individual defendants fails because no predicate claim under Section 10(b) has been stated.

VI. CONCLUSION

Having failed to allege a materially false or misleading statement, plaintiff's claim under Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder must be dismissed. Moreover, plaintiff's failure to plead a primary violation of Section 10(b) requires the dismissal of the Section 20(a) claim against the individual defendants.

Based upon the foregoing, defendants' motion to dismiss the CCAC is **GRANTED**. Although the Court harbors doubts that plaintiff can cure the deficiencies outlined above, in an abundance of caution, and because the Court has not provided plaintiff with a prior opportunity to amend,[19] plaintiff is given **LEAVE TO AMEND**. Plaintiff shall file an amended complaint within **twenty-eight (28) days** from the date of this Order. Defendants shall file responsive pleadings within **twenty-eight (28) days** after service.

This Order terminates Docket Number 67.

IT IS SO ORDERED.

Dated: March 29, 2019

YVONNE GONZALEZ ROGERS
UNITED STATES DISTRICT COURT JUDGE

[19] Defendants note that plaintiff has already amended its complaint once. *See* MTD at 25. While this is technically true, this is the first time the Court has assessed the sufficiency of plaintiff's allegations.

APPENDIX A

1. Statements Published on Intel's Website "Throughout the Class Period"

a. Statements regarding the Company's Intel® Core™ processors

A new computer with a new 8th Generation Intel® Core™ processor helps you stay ahead of the digital world. ***Get a big jump in performance*** compared to the previous generation. Experience vivid gaming and content creation, immerse yourself in leading-edge 4K UHD entertainment.

Get Unprecedented Power and Responsiveness
Now everyday computer tasks can happen faster. Edit photos and videos seamlessly. Move between programs and windows quickly. ***Multitask easily. Better still, all that performance comes with up to 10 hours of battery life*** . . .

Easy to Use, Hard to Break Into
Built-in security adds a critical layer of protection to make password logons, browsing, and online payments ***safe and simple***. You can log on with a look, your voice, or your fingerprint for ***rock-solid security*** that's fast and hassle free. Store passwords, personal information, and auto-fill information with one master password. Plus touch screen, voice commands, and stylus options offer natural and intuitive interactions.

(CCAC ¶ 132.)

b. Statements regarding the Company's Intel® Core™ X-series processors

Features At-a-Glance

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI). A fast, secure AES engine for a variety of encryption apps, including whole disk encryption, file storage encryption, conditional access of HD content, ***internet security,*** and VOIP. ***Consumers benefit from protected internet and email content, plus fast, responsive disk encryption.***

(*Id*. ¶ 134.)

c. Statements regarding the Company's 8th Gen Intel® Core™ i7 processors

Get Unprecedented Power and Responsiveness
Now everyday computer tasks can happen faster. Edit photos and videos seamlessly. Move between programs and windows quickly. Multitask easily. Better still, all that ***performance comes with up to 10 hours of battery life,*** so you can take your computer wherever you go without worrying about cords and plug

points.

Easy to Use, Hard to Break Into
Built-in security adds a critical layer of protection to make password logons, browsing, and online payments safe and simple. You can log on with a look, your voice, or your fingerprint for ***rock-solid security*** that's fast and hassle free. Store passwords, personal information, and auto-fill information with one master password. Plus touch screen, voice commands, and stylus options offer natural and intuitive interactions.

Intel® Online Connect
With Intel® Online Connect, ***security is built-in 7th Generation Intel® Core™ processors and above***, which adds a ***layer of protection*** to make browsing and online payments safe and simple.

(*Id*. ¶ 136.)

d. Statements regarding the Company's 8th Gen Intel® Core™ i7 processors

Prepare To Be Amazed With The 8th Generation Intel® Core™ Desktop Processor Family

DISCOVER THE BENEFITS

1 - ***Exceptional platform performance*** with up to six cores for more processing power
. . .
3 - ***Hardware-level technologies that strengthen the protection of enabled security software***
. . .

Ultimate Protection Built Into the Silicon
8th Generation Intel® Core™ processors integrate hardware-level technologies that strengthen the protection of your ***enabled security software. Hardware-based security*** helps you experience online and offline activities with peace of mind, enabled by features that include:

- Intel® Software Guard Extensions (Intel® SGX) to help applications protect your system and your data
- Intel® BIOS Guard and Intel® Boot Guard to help protect your system during startup

(*Id*. ¶ 138.)

///

///

///

///

e. Statements regarding the Company's 7th Generation Intel® Core ® vPro™ processor

Performance That Unleashes Productivity.

Security That's Hardware-Enhanced.

7th Generation Intel® Core® vPro™ processor
. . .
Hardware-Enhanced Security

Built-in protection runs deeper than just software.
63% of data breaches start with misused or stolen credentials. Intel Authenticate Solution provides a robust multifactor verification solution that is protected in hardware, reducing exposure to software-level attacks
. . .
Multifactor verification.
Customize your policy to protect against today's most common threat with multiple factors, including protected PIN, Bluetooth technology proximity, fingerprint, and location detection using Intel Active Management Technology (Intel AMT).

(*Id*. ¶ 140.)

f. Statements regarding the Company's Intel® vPro™ platform

Explore how Intel® vPro™ platform business solutions increase productivity, improve manageability, and ***provide security*** for business transactions. Learn more about how this platform improves performance by creating faster multitasking ***with optimal data security***. This easily deployable business platform creates a stable environment that will keep your business up and running smoothly.

Performance
The latest Intel Core vPro processors…. Results in amazingly responsive systems that increase productivity for all workers.…

Security – Hardware-Enhanced Data Encryption ***Intel Data Guard technology***
Hardware-Enhanced Identity Protection ***Intel Authenticate Solution***

(*Id*. ¶ 142.)

g. Statements regarding the Company's Intel® Xeon® Scalable processors

- Take a Major Leap Forward
  New Intel® Xeon® Scalable processors are workload-optimized to support hybrid cloud infrastructures and the most high-demand applications. You can drive actionable insight, ***count on hardware-based security***, and deploy dynamic service delivery.

Advanced Features Are Designed into the Silicon
Synergy among compute, network, and storage is built in. ***Intel® Xeon® Scalable processors optimize interconnectivity with a focus on speed without compromising data security***. Here are just a few of the value-added features:
. . .
Improve Security

Deploy hardware-enhanced security to protect data and system operations without compromising performance.

(*Id*. ¶ 144.)

- Create a Silicon-Based Trusted Infrastructure

The Intel® Xeon® Scalable platform delivers an essential, hardware-based root-of-trust environment. Protection extends up from the silicon, through the platform hardware and firmware, ensuring an effective IT security platform

Ensure Trust, Resilience, and Control

Intel® technology enables Trusted Infrastructure through a suite of platform security technologies built into Intel® silicon. ***Hardware-based security technologies provide a critical foundation for secure IT. They address the numerous, increasing, and evolving security threats across physical and virtual infrastructures***.

(*Id*. ¶ 146.)

h. Statements regarding the Company's Intel® Xeon® E3 processors

Intel® Xeon® E3 processors deliver ***essential performance*** and visuals to support the needs of businesses worldwide, including: small business servers, powerful mobile workstations, entry workstations, storage servers, cloud workstations, media transcode and edge computing/IoT.

Professional Workstations
Step up to the ***essential performance*** and visuals demanded professional CAD and media workstation customers. Experience the difference of ***professional-grade compute performance*** with enhanced memory capabilities, ***hardware-enhanced security***, and reliability features and support for the latest Intel graphics.

Reliability for Small Business
No matter what the size of your business, the value of your data is enormous. ***Keep it accessible and better protected***, with ***hardware-enhanced performance***, at all times, with an affordable Intel® Xeon® E3-1200 v6 processor-based small business server.

(*Id*. ¶ 148.)

i. Statements regarding the Company's Intel® Xeon® processor E3 v3 family, the Intel® Xeon® processor E5 family, and the Intel® Xeon® processor E7 family

Data Protection with Harware-Assisted Security

Ensuring Data Protection Through Innovation

The rapidly expanding dependence on computing devices creates the need for more secure software and hardware products for businesses and consumers to prevent exposure to malicious code, viruses, cyber espionage, malware, and data theft. This is also one of the drivers behind the rapid growth in cloud computing architectures for enterprises and consumers alike.

The hosting and scaling of data centers into cloud infrastructures creates new security challenges and risks for businesses and consumers. While cloud technologies promise to bring automation and agility to data center operations, they also challenge many of the underlying traditional security tools and physical control once enjoyed by IT. New tools are needed to address growing security challenges, such as establishing visibility to the state of the servers and assuring data confidentiality in the cloud and virtualized data centers—especially for missioncritical or sensitive data or workloads.

Intel continues to enhance systems so they run more securely. A key component of this approach is providing ***more robust, vulnerability-resistant platforms***. Security features are embedded in the hardware of Intel® processors, including three of Intel's newest server processors—the Intel® Xeon® processor E3 v3 family, the Intel® Xeon® processor E5 family, and the Intel® Xeon® processor E7 family, as well as the latest generation Intel® Core™ vPro™ processors.

(*Id*. ¶ 150.)

j. Statements regarding the Company's Intel® Pentium® and Celeron® processors

Intel® Pentium® and Celeron® Processors

DISCOVER THE BENEFITS

1 - Enjoy more computing and greater graphics longer
2 - Uncompromised user experience at entry system price
3 - ***Security you can trust***
4 - Choose from a wide range of mobile form factors

With up to ***30% more processor performance*** and 45% better graphics on Windows than the previous generation platform, the latest **Intel® Pentium® and Celeron® processors** give your platform the computing and visual power you've wanted.

Security You Can Trust
Protection capabilities in the **Intel® Pentium® and Celeron® processors** are built from the ground up to give you a device you can trust. Every time you start it up, ***secure boot*** with Intel® Platform Trust Technology helps keep your ***device safe, blocking dangerous programs***, so only trusted software is launched. You get peace of mind with a ***more secure operating environment***. Execute Disable Bit defends against ever-elusive malware, reducing your exposure to viruses and malicious code attacks. It works behind the scenes, so you don't have to think about it, and it shuts down malicious code before it can take root.

It's ***easy to secure all your data*** with Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) new instructions built into the processor. You get ***strong security without compromising performance or impacting your experience.***

(*Id*. ¶ 152.)

2. October 26, 2017 3-Q Results

On October 26, 2017, four days before Defendant Krzanich modified his 10b5-1 plan, Intel filed with the SEC its quarterly report for the third quarter of fiscal 2017 on Form 10-Q. In the section titled, "Management Discussions and Analysis of Financial Conditions and Results of Operations," Intel stated, "During the quarter, we launched our 8th Generation Intel® Core™ Processors, code named Coffee Lake, ***which delivered significant performance improvement to our client platforms.***"

(*Id*. ¶ 154.)

That same day, Defendants held a quarterly investor conference call during which Defendant Krzanich stated, "We're especially excited about the launch of our latest Eighth Generation Core processor, codenamed Coffee Lake. The Coffee Lake family includes our first 6-core desktop CPU. And it's our best gaming processor to date, ***with up to 50% better performance than the competition on top-game titles***."

(*Id*. ¶ 155.)

3. October 27, 2017 Intel Publication – Unlocking Data Insights with the Powerful Intel Xeon Scalable Processor

On October 27, 2017, Intel published on the Company's website an article titled "Unlocking Data Insights With The Powerful Intel Xeon Scalable Processor," which focused on Intel's recent launch of the Intel® Xeon® Scalable processor. In the article, Defendants stated, "The recently launched Intel® Xeon® Scalable Processor family provides powerful performance for the widest variety of workloads, including ***a 1.73X average performance boost*** vs. the previous generation across key industry-standard workloads. Architected with increased memory and IO bandwidth, as well as ***advanced security features***, Intel Xeon Scalable Processors are optimized to deliver 2.2X higher deep learning training and up to ***2.4X higher inference performance*** compared to the prior generation."

(*Id*. ¶ 157.)

4. November 14, 2017 UBS Global Technology Conference

- On November 14, 2017, Defendant Shenoy presented at the UBS Global Technology Conference. During that conference, Defendant Shenoy offered a Company Investor Relations Presentation, where on slide 9, Defendants stated,

  "Intel Xeon Scalable Processor
  Leadership vs. other x86 offerings 34% more performance, 53% more perf. Per core 18% more perf. Per watt."

  (*Id*. ¶ 159.)

- During the conference, Shenoy made further statements regarding the Xeon® Scalable platform, including:

  This represents -- this product, the Xeon Scalable Skylake platform -- represents the biggest advancement that we've delivered in about a decade in terms of generation on-generation performance gains. We delivered about a 1.65x improvement gen-on-gen. I mean, that's more than we would typically do in a gen-on-gen advancement.

  And so I wanted to show you a couple of charts to demonstrate the performance leadership we believe we have. This Xeon architecture, of course, has been in the market for over 20 years now. It's proven. It's very much battle tested. ***It has outstanding performance on a wide range of workloads that are designed to optimize not only performance but security and agility of various workloads in the data center***.

  The chart on the top shows the Xeon Scalable versus other x86 offerings in the marketplace. Using published benchmark data, we believe that Xeon Scalable outperforms on throughputs kind of benchmarks by 34%, by 18% on performance per watt benchmarks and by over 50% on performance per core, which is an important metric when you talk to the cloud service providers, when you talk to software companies because they are deploying, in many cases, on a multicore environment, and they want to know what does my per-core performance look like.

  (*Id*. ¶ 160.)

5. November 28, 2017 Credit Suisse Technology, Media, and Telecom Conference

On November 28, 2017, Defendant Swan presented at the Credit Suisse Technology, Media and Telecom Conference. During the presentation, Swan discussed the intersection of client demand for Intel's products versus the performance of those products, stating:

Question– John William Pitzer: In the core servers Xeon business, how important are product cycles? And I probably get 14 or 15 questions a week about Purley and sort of how Purley is sort of unfolding and kind of what's the outlook there. So can you talk a little bit about product cycle importance in general and specifically how you see Purley rolling out over the next 4 to 6 quarters?

Answer – Robert H. Swan: I think I'm going to focus a little bit on the cloud, if you don't mind, and if you -- I think -- but I think it applies for enterprise as well. ***This is a -- where everyone, all the CIOs, are dealing with this increasing demand to be more efficient but to also deal with more cybersecurity threats. The demands of their internal customers to get more access to more data, to analyze it more effectively are growing and growing and growing***. And they have -- their demands for compute memory and storage are growing like crazy. And in that world, you have -- they don't all want to just pay X percent. If they have 30% more demand for data, they don't want to pay 30% more for that performance. So what they're looking for, CIOs in general, whether they offload to the cloud or perform on-premise, they're looking for more performance to deal with the increasing challenges that they're facing with. So that more performance comes from just a more predictable cadence of new products that deliver higher performance. And so that's -- we're trying to continue, much like we are in the client side, just an annual rollout of products that can deliver higher performance so they can deal with the increasing demands of what data means for their collective spending envelope. It's very important. Purley is our most recent new product launch, as you know, with dramatically improved performance suite. We launched it in the July time frame. And it's got -- it's just -- it's grown now -- it'll grow over the course of -- you got to kind of slot it into their replacement cycles so we don't launch the product and they say, oh, let's go replace everything, but it's been growing over the course of the third quarter. And we expect, as they go through their refresh, the demand for this higher-performance product will continue to grow and will be a source of growth for us in kind of the fourth quarter into 2018.

(*Id*. ¶ 162.)

6. December 5, 2017 Intel Corp at Nasdaq Investor Program

On December 5, 2017, Venkata Murthy Renduchintala, Intel's Chief Engineering Officer and President of Client & Internet of Things Businesses & Systems Architecture presented the Nasdaq Investor Program. During the conference, Intel touted its Core platforms' performance, stating, ***"[I]f you do a like-by-like performance, from the first product in 14, Broadwell, for example, to the eighth generation Intel device, we've seen an over 30% improvement in the performance of the devices. And that's just a testament to how much intra-node benefit there is.***

(*Id*. ¶ 163.)

///

///

7. December 20, 2017 Intel Hardware-Based Security Video

On December 20, 2017, Defendants posted a video entitled, "Endpoint Security at the Hardware Level" on the Company's website. In the video, Yasser Rasheed, Global Director of Business Client Security at Intel, states:

> Software attack versus software protection, this is a race, a race between the good and the bad. There are 4 priorities that IT needs to keep in mind: identity protection, data protection, threat detection, and prevention and recovery from breaches; at the end of the day end users will always opt for what's simpler and what makes them productive and they will deprioritize what makes them more secure. IT needs to now make it simpler and easier for end users to be productive and on the back end add the right infrastructure for auditability, compliance and so on. Hardware-based protection makes it exponentially harder for the attackers to get in. ***We have the ability to protect against identity breaches with multi-factor authentication in the hardware protecting the factors, the policy and the credentials. At Intel we believe we have an opportunity to bring in hardware-based protection in such a way that protects the good people from the bad people***.

(*Id*. ¶ 167.)